(12) UK Patent Application (19) GB (11) 2 317 476 (13) A

(43) Date of Printing by UK Office 25.03.1998

(21) Application No 9800437.7

(22) Date of Filing 08.07.1996

(30) Priority Data
(31) 50411795 (32) 19.07.1995 (33) US

(86) International Application Data
PCT/US96/11416 En 08.07.1996

(87) International Publication Data
WO97/04412 En 06.02.1997

(51) INT CL^6
G06F 12/14 1/00

(52) UK CL (Edition P)
G4A AAP

(56) Documents Cited by ISA
US 5379342 A US 5212729 A US 5083309 A
US 4959861 A US 4944008 A

(58) Field of Search by ISA
US Classification: 380/ 25, 4

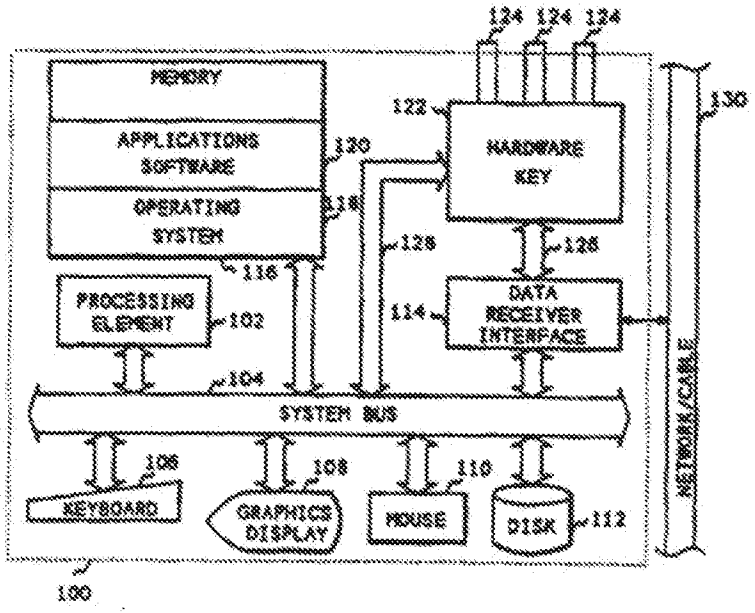
(71) Applicant(s)
Cable Television Laboratories Inc.
400 Centennial Parkway, Louisville,
COLORADO 80027-1208, United States of America

(72) Inventor(s)
Thomas H Williams
Claude T Baggett

(74) Agent and/or Address for Service
Saunders & Dolleymore
9 Rickmansworth Road, WATFORD, Herts, WD1 7HE,
United Kingdom

(54) **Method for protecting publicly distributed software**

(57) A system for protecting software from copying wherein the software to be protected is placed on the computer system in two parts. A first part (120) is stored in non-volatile storage, such as a hard disk or floppy disk within the computer system (100), and a second part is stored and executed in a "hardware key (122)", which is attached to the computer system (100). The second part is stored in volatile RAM (206) and will be erased when electrical power is removed from the hardware key (122), or when the software stops execution. This requires that the second part of the software be reloaded each time the hardware key (122) is powered up. Typically, the second part of the software will be loaded from a network (130), or from a cable network, thus reloading of the second part into the hardware key (122) is a trivial matter, so long as the user is an active subscriber to the network (130) or cable network.



GB 2 317 476 A

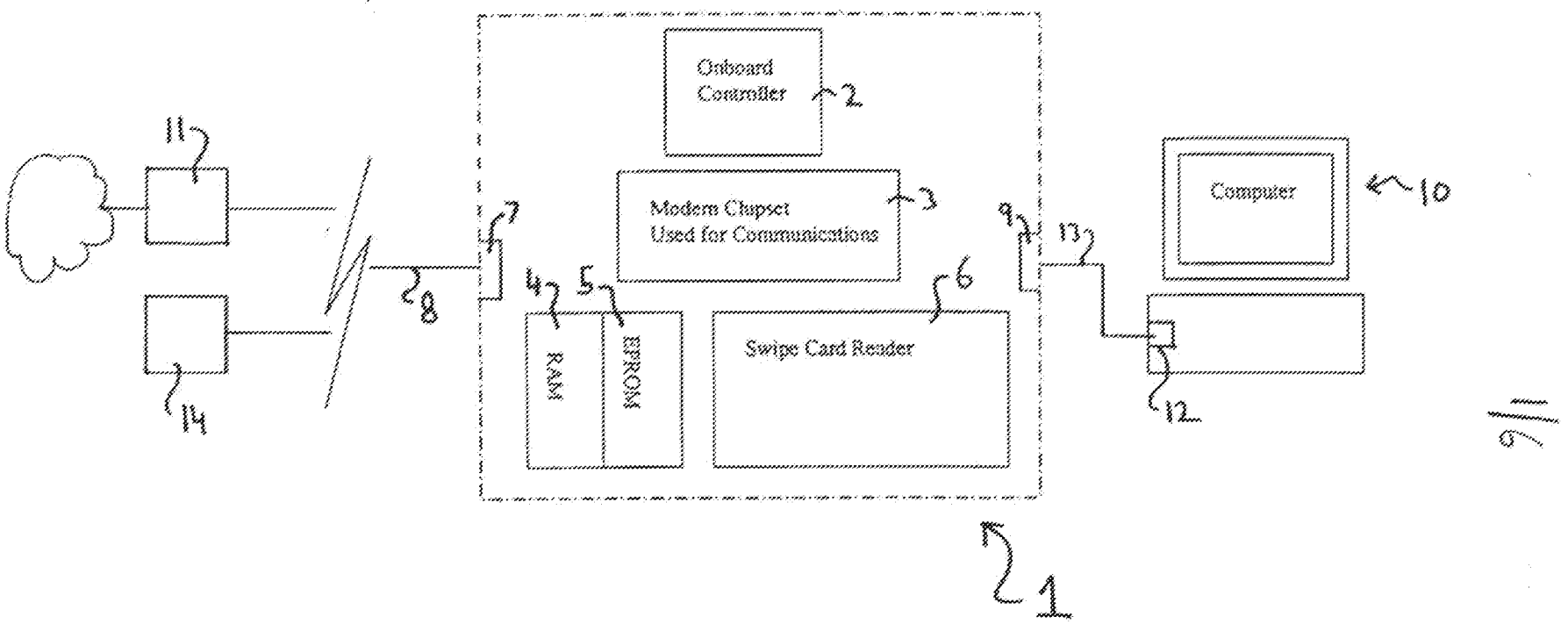

Onboard Controller
2
Modem Chipset Used for Communications
3
RAM
4
EPROM
5
Swipe Card Reader
6
7
8
9
11
12
13
14
Computer
10
1

Fig 1

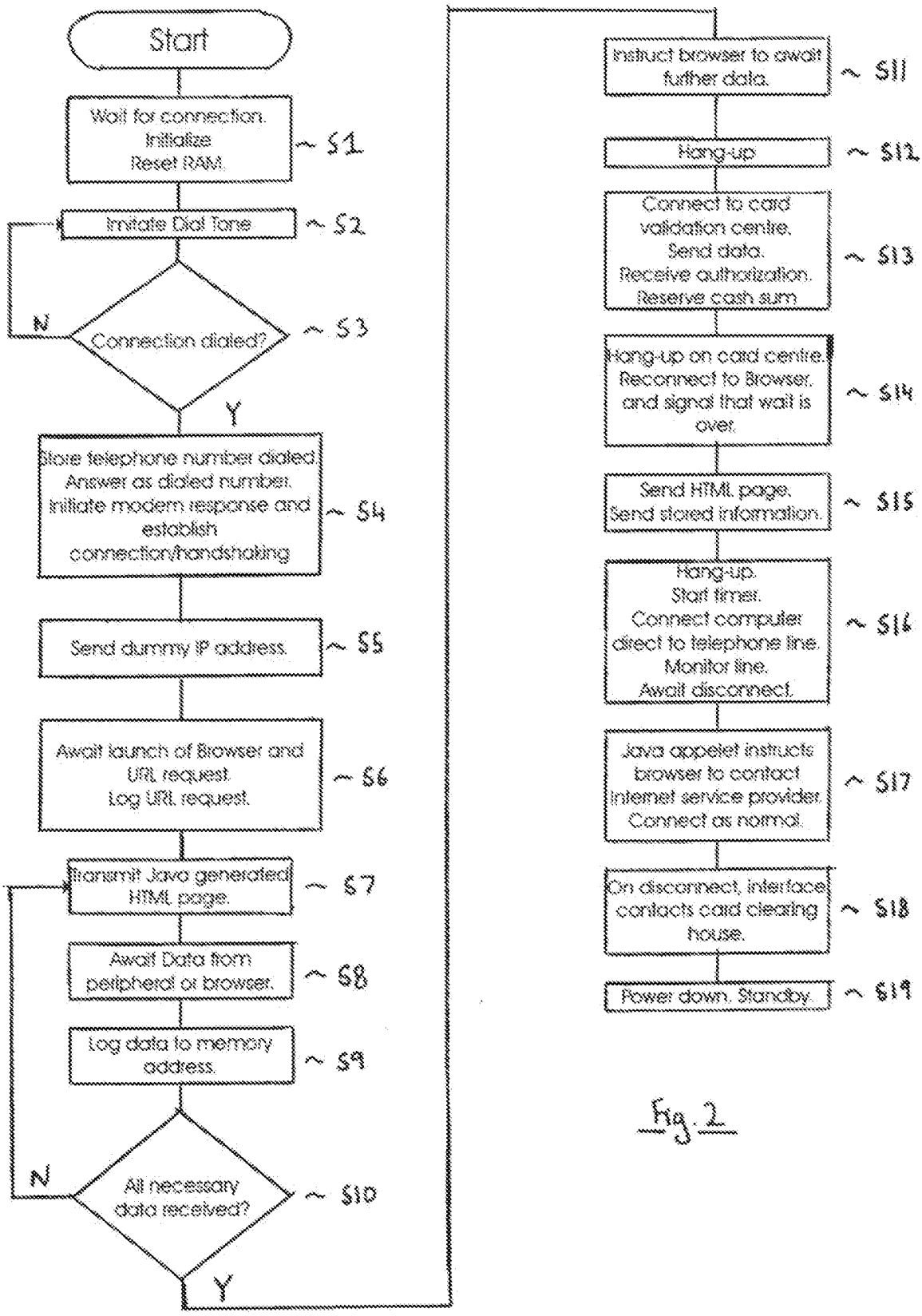

Start
Wait for connection.
Initialize
Reset RAM.
S1
Initiate Dial Tone
S2
N
Connection dialed?
S3
Y
Store telephone number dialed.
Answer as dialed number.
Initiate modem response and
establish
connection/handshaking
S4
Send dummy IP address.
S5
Await launch of Browser and
URL request.
Log URL request.
S6
Transmit Java generated
HTML page.
S7
Await Data from
peripheral or browser.
S8
Log data to memory
address.
S9
N
All necessary
data received?
S10
Y
Instruct browser to await
further data.
S11
Hang-up
S12
Connect to card
validation centre.
Send data.
Receive authorization.
Reserve cash sum
S13
Hang-up on card centre.
Reconnect to Browser,
and signal that wait is
over.
S14
Send HTML page.
Send stored information.
S15
Hang-up.
Start timer.
Connect computer
direct to telephone line.
Monitor line.
Await disconnect.
S16
Java applet instructs
browser to contact
internet service provider.
Connect as normal.
S17
On disconnect, interface
contacts card clearing
house.
S18
Power down. Standby.
S19

Fig. 2

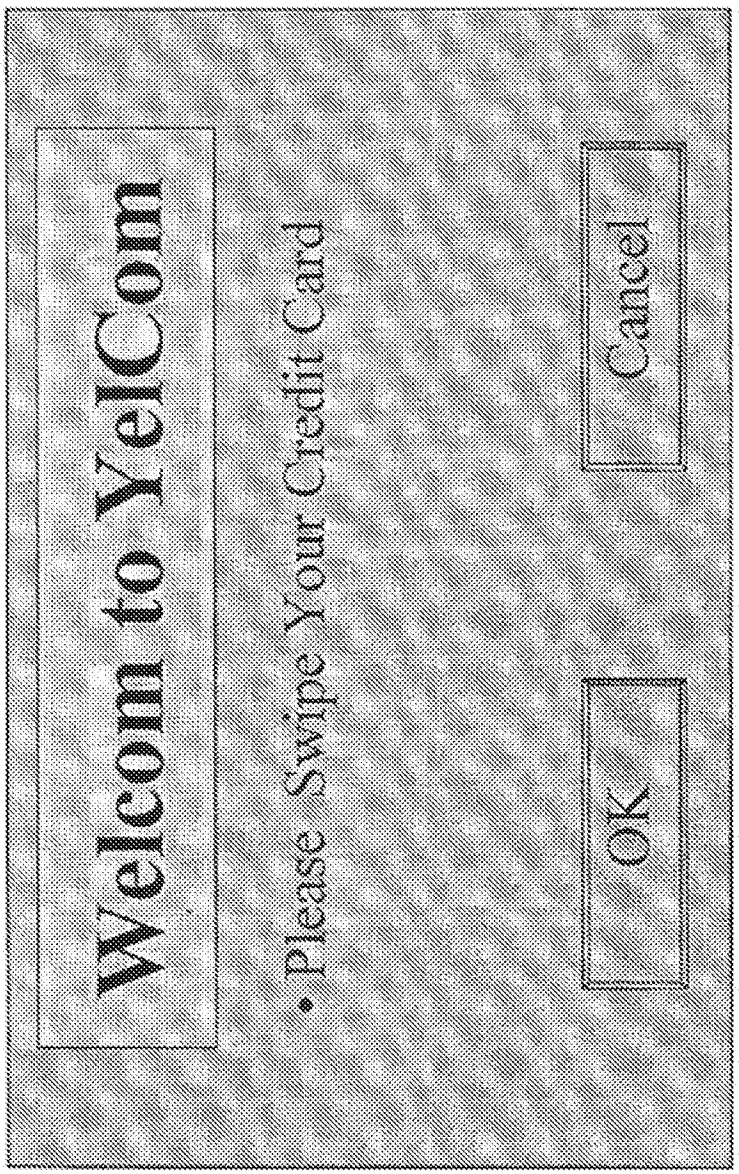


Fig. 3

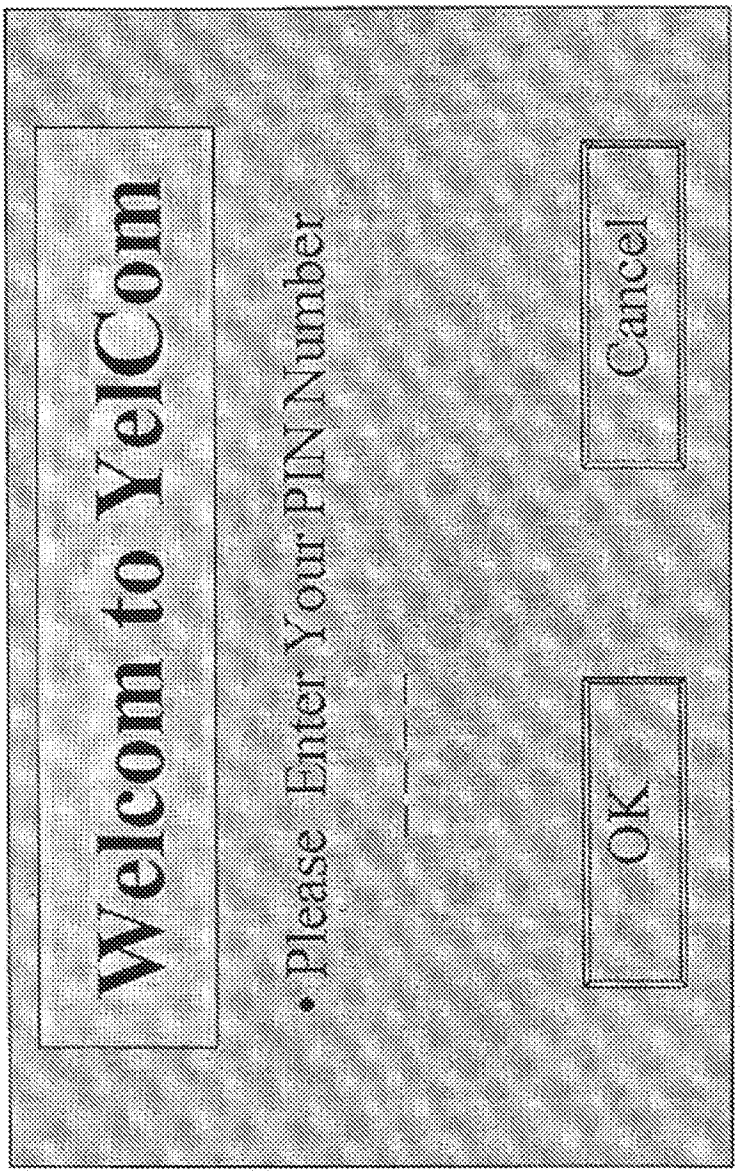


Fig.4

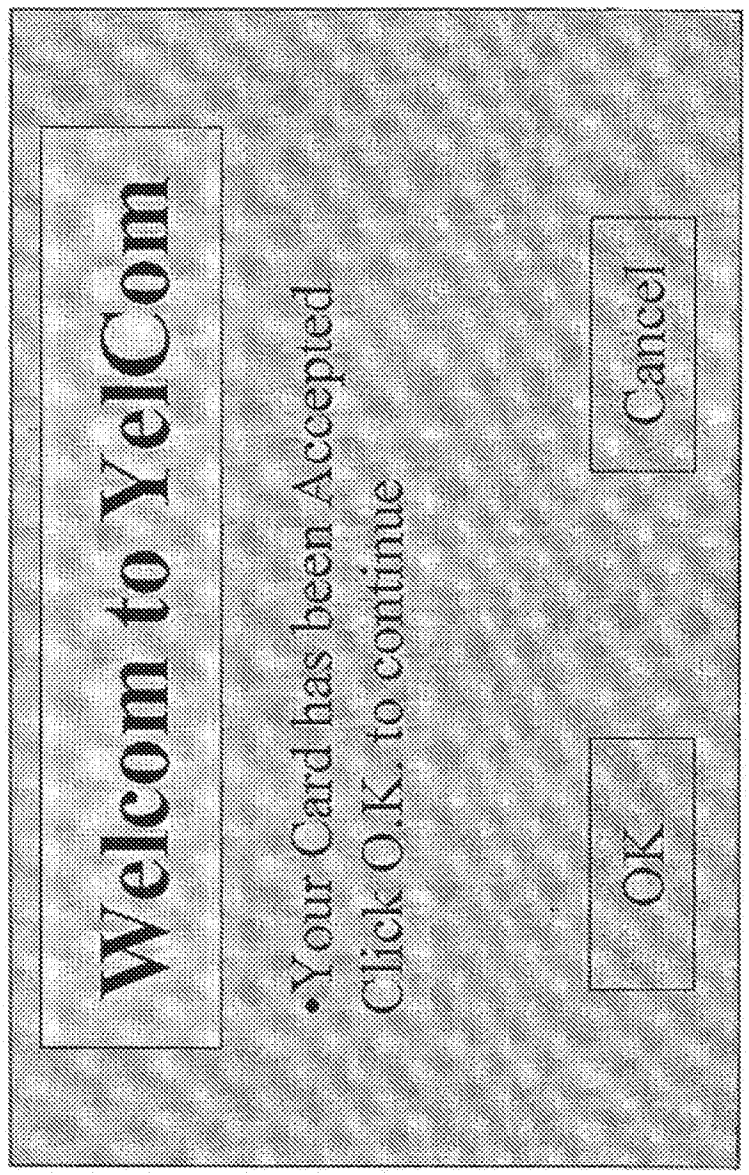

Welcom to YelCom
•Your Card has been Accepted
Click O.K. to contime
OK
Cancel

Fig. 5

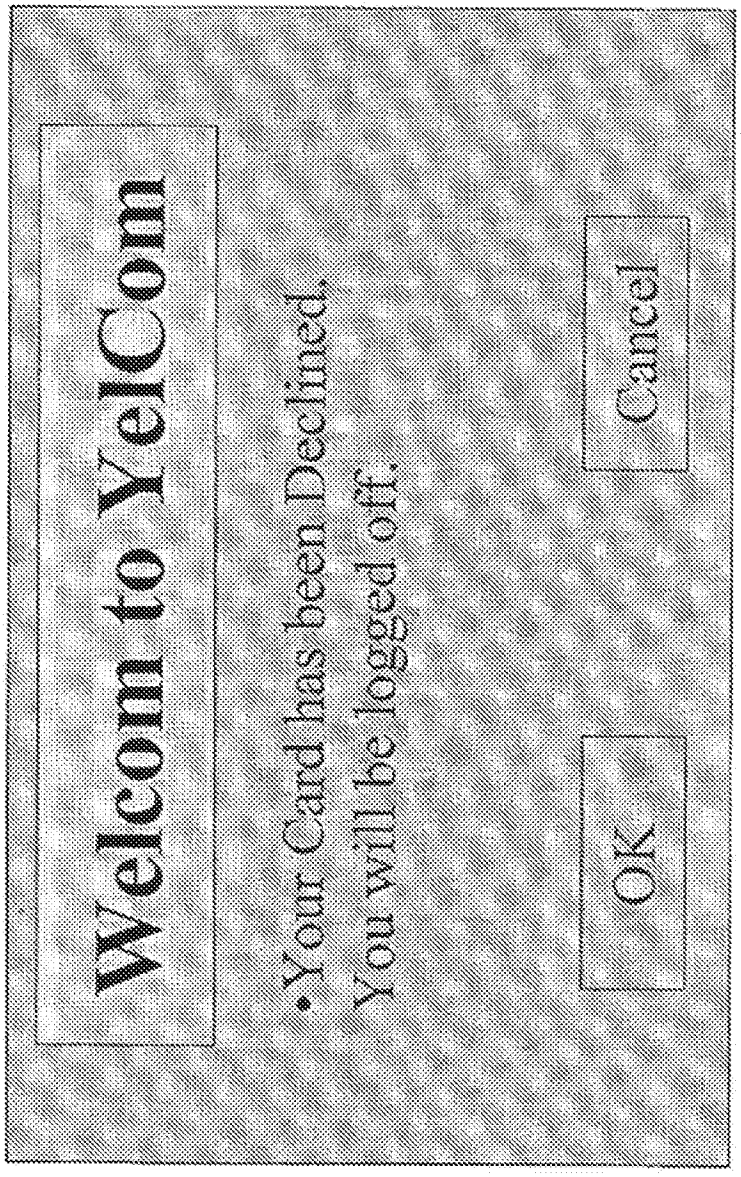

Welcom to YelCom
•Your Card has been Declined.
You will be logged off.
OK
Cancel

Figure 4

Apparatus and Method for Allowing Connection to a Network

The present invention relates to an apparatus and method for connecting a computer to a network such as the Internet or an intranet.

One object of the present invention is to allow a connection to the network only if the user is suitably authorised to do so. For example if they are able to pay for the connection using a valid credit card or are security cleared.

Viewed from one aspect, the present invention provides interface apparatus for allowing a computer to connect to a network, wherein the apparatus in use mimics a connection to the network by the computer so that the computer is able to launch a browser application for the network, the apparatus downloading a program or other coding (e.g. a html page) to the computer to be run/interpreted by the browser to obtain validation data from the user, the computer being allowed access to the network when the validation data is determined to be valid.

The validation data may take any suitable form, and in an especially preferred embodiment, may be data associated with a credit, debit or other such card, in which case the apparatus may include means for reading the card, such as a swipe card reader for magnetic media. The data from the card is then able to be checked, e.g. against data input by the user (e.g. through the keyboard) to check that the user is a valid user. For a magnetic swipe card the input data may be a PIN number (personal identification number).

The interface apparatus thus may allow a user to access a network such as the Internet or a company intranet on payment of a fee through the credit card or allow suitably authorised individuals onto an intranet.

The use of the computer's browser interface to obtain the validation information from the user enables the interface to be small and inexpensive. The interface may run a small operating system, such as a Linix/Linux operating system, doslite or RomDos or the like, and may run a Java application in use.

In a preferred embodiment, a validation centre may be dialled for a validation of the user. This connection is preferably made by the interface apparatus itself, but might possibly be made by the computer's modem on the instructions of the program/coding downloaded to the computer.

In one embodiment, the validation centre may be a credit card clearing or debit card organisation. The user may then pay for access to the network, e.g. on a one time payment per session basis or on a time basis. In the former case, the connection may be terminated after a set time. In the latter case, the interface apparatus or computer may time the duration of the network connection and may reconnect with the centre at termination of the session in order to confirm the cost incurred, so that a suitable billing may be made on the card.

It would be possible to call the clearing organisation only after the network connection has finished. This might however increase the chances of a fraudulent use of the card and also runs the risk of the card being over its credit limit.

In a preferred embodiment, when the apparatus contacts a card validation centre, it reserves an amount of credit on the card which corresponds to a predetermined amount of time on the network. The session will then be terminated either by the user before the predetermined time has expired or by the apparatus when the predetermined time has elapsed. In either case, the card centre is then contacted and a charge is made on the card corresponding to the duration

of the session and in accordance with a tariff which may be set by the owner of the interface apparatus in order e.g. to obtain a suitable profit. This embodiment has the advantage that the reservation of a credit amount ensures payment for the time which the user has been on the network. The amount of credit reserved may be high enough so that users will generally not be interrupted by a time-out of the apparatus.

Rather than being a credit card clearing centre, the validation centre could be a centre for a charge card or the like specific to a particular company, e.g. a user might buy time on the Internet using a dedicated charge card, and would be allowed onto the Internet for up to the pre-bought time remaining on the card. Alternatively, the time for which the user is on the Internet is recorded and billed at an appropriate time, e.g. at the end of a month.

In a further alternative embodiment, the centre may be a security centre, e.g. of a company having its own intranet to which the computer is attempting to connect. The centre may have details of valid and invalid cards, and so may advise the apparatus as to the status of the user requesting the access. This embodiment may also help in internal account controls of a company, by allowing charges to be assigned to particular company departments, with respect to e.g. telephone charges allowed per department.

The security centre could also hold verification data which the interface apparatus obtains from the computer user via the computer and which the apparatus passes to the security centre for verification. In this embodiment, therefore, no card would be needed, as the program which the apparatus downloads to the computer could merely prompt the user for the verification data stored at the centre.

Other validation data, besides magnetic card data, may be used. For example, a smart card with a microchip

therein may be used or physical characteristics, such as palm or finger prints or an eye scan. The swipe reader may then be replaced by a suitable reader for the validation data used.

In order to initially mimic the network which the computer is attempting to access, the apparatus may respond to the computer in any suitable manner.

As connection is generally by a modem, the apparatus will initially present a dial tone to the modem when the modem is connected to it.

Where the network is the Internet, the computer will attempt to dial a service provider on starting the dial-up networking routine. The apparatus of the present invention replies as if it is a modem of the service provider, and carries out the necessary protocols and hand-shaking with the modem to establish a connection. This may include the provision of an IP address to the computer to allow the browser to launch, as well as the capture and storage of a user's username and password for the network.

In a preferred embodiment, the initial IP address sent to the computer is a dummy one which is used only to allow the browser to launch, the computer being assigned a new IP address on eventual connection with a service provider. In an alternative embodiment, where the interface apparatus is tied to one service provider, it may be possible to have a dedicated IP address for the interface apparatus which the computer retains on access.

The browser is then launched by the user and an URL request will be sent out by the browser. This may not happen straight away, as the user's home page may for example be set to a page stored on their hard disc. However, as soon as access to the Internet is required, an URL request will issue from the browser, and the interface apparatus will intercept this and preferably store it for future use. The interface apparatus will

then send e.g. one or more html pages (hypertext format information files) to the browser interface to prompt a request for for example a swipe of the user's card, e.g. credit card, and the input of the user's validation data, e.g. their PIN number. In each case, the interface may be directed to look for feedback from a suitable source, e.g. either data from a card reader or other peripheral of the interface or data sent by the computer's browser.

The interface may also download e.g. a Java appelet to the browser interface to control the operation of the interface during later stages of the connection procedure.

Once all of the required information has been received for validation, the interface may then hang-up its connection with the computer and connect with a card clearing centre. At this stage, the computer browser will have been given instructions to await further information. It therefore waits in a standby mode for further data from the interface on reconnect. The above-mentioned appelet controls the various browser operational instructions for this procedure.

Where the network is an intranet, the computer may send out an URL request corresponding with the address of one of the intranet's externally accessible pages, and passwords and usernames may be necessary.

Once the user is considered to be a valid user, the apparatus may then allow the computer to connect to the actual network. The connection is preferably made with the modem of the computer.

The interface will hang-up its connection with the clearing house, and then reconnect with the computer, which has been waiting for further information. A html page may then be downloaded to confirm that access to the network is being allowed or denied, and information necessary to log onto the network, such as the previously stored username and password may also be

downloaded. The browser then hangs up the connection in accordance with the appelet and dials out to connect to the Internet as normal. The interface may switch e.g. a relay to allow for normal access to the telephone system.

If the network is the Internet, the computer connects to either the service provider initially called by the user or to a service provider associated with the socket (a telephone number for which may be stored in the interface apparatus). The browser may then connect either with the URL requested by the user or with an URL address that may be stored in the interface apparatus. This latter address could for example be an advertisement or welcome page to a service provider associated with the interface apparatus or the home page of the organisation which operates the interface apparatus. This page may provide the option of proceeding to the originally requested page. These connections may be made by the browser following the instructions of the above-mentioned appelet downloaded at the start of the connection, and by using the username, passwords, etc., stored by the interface apparatus and subsequently downloaded to the browser.

Once connected to the service provider, the computer may then have unrestricted access to the Internet through this provider.

Where the network is an intranet, the apparatus may connect the computer to the intranet at the appropriate front page URL address of a company's intranet server.

The interface apparatus preferably monitors the network connection, e.g. it times the duration of the connection, and awaits termination of the session, e.g. by a time-out or by the user hanging up the call. Once the session is terminated, a further connection to a credit card clearing organisation or some other such service may be made by the interface apparatus to for example bill the credit card for the appropriate amount.

The apparatus may be provided as a socket on a wall, so that it appears e.g. as a normal telecommunications socket for a telephone, with preferably a card swipe mounted to or adjacent it. Alternatively, it may be provided as a stand alone unit which must be connected with both the computer and a telephone socket. In a further form, the apparatus may be mounted within the computer itself, e.g. as an add-on card.

The interface apparatus may be especially useful in for example hotels and conferencing facilities, where for example a bank of such interface sockets may be provided. A user need then only connect their computer to one of the sockets and begin work, whilst being billed directly through their credit card and without the need for example to have a room number against which their call to the service provider can be billed. The interfaces may be used in any suitable establishments, such as cafes, which provide Internet access on payment of a fee.

The charges made on the credit card may be e.g. by the hotel or conference centre providing the interface, and may include the telephone line time charge at a standard rate or at a rate increased to provide some profit to the socket provider, as well as a fee for the use of the socket. A charge may also be made by a service provider associated with the socket for e.g. online time and/or a connection fee.

The apparatus may comprise an onboard controller which overseas the operations of the apparatus, and a standard modem chipset used for establishing connections with the computer. It may also comprise RAM for storing information from the user such as the original destination dialled, the user's username and password and any URL requested, as well as data from the card swipe. An EPROM or other updateable memory may hold the program for the controller and the program, pages,

appelets or other coding for downloading to the computer, so that these programs may easily be updated down the network line, e.g. telephone line, to which the apparatus is connected. This may allow for example simple change of charging tariffs, so that the owner of the interfaces may increase e.g. the cost per unit time of the connection.

In a particularly preferred embodiment, the modem chipset of the interface apparatus is only used in connecting and communicating with the computer, and preferably also to connect with a validation centre at the start and end of the network connection. In contrast, the connections to the service provider are preferably carried out by the modem of the computer. This means that the levels of for example the speed, data compression, error checking and protocols of the connections are determined by the computer modem and not by the interface modem chipset. This then allows the interface modem chipset to be relatively inexpensive as it does not need to be particularly fast - the connection between the computer and the interface is a relatively short distance and the amount of information transferred e.g. to a card clearing centre is also relatively small, and so a slow modem will not affect the performance of the interface. It also means that there will be no need to upgrade the interface to keep up with changes in modem specifications, etc. This does not exclude however the possibility of the modem software being upgradable especially by a download of new software e.g. to a flash memory.

In order to allow the computer to connect to the clearing centre and service provider, the appelet downloaded to the computer from the interface should include instructions for telephoning the clearing centre and the service provider. If the user is to connect to their own service provider, then the interface apparatus should also download e.g. the initial telephone number

dialled and the captured username and password to the computer for use by browser run appelet. Alternatively, if a default service provider is to be used, the appelet will already have the service provider number and a suitable username and password (e.g. guest), and the only information necessary to be re-sent to the computer from the interface will be possibly a URL which was initially requested by the browser.

The program or other coding which is downloaded to the computer by the interface apparatus may be in the form of a HTML/world wide web page comprising programs embedded as e.g. JAVA™, JAVASCRIPT™, and/or ACTIVEX™ appelets.

The prompt for information from the user may comprise a web page form which the user completes with the necessary information.

If the card is not validated, then a card rejection screen may be produced on the computer display, and the connection will be terminated by the apparatus. If the card is accepted, then a screen may appear stating that the card has been accepted and that the user may now connect with the network.

If e.g. the PIN number does not match the card number, and authorisation is denied, then the interface may still allow access to the network, whilst also notifying suitable authorities, to allow time for the user to be apprehended.

The apparatus may be configured so as to work on any suitable communications line, for example on a standard POTS line or on an ISDN line.

The invention also extends to a method of allowing the connection of a computer to a network by providing an interface between the computer and the network, the interface enabling validation information to be obtained from the user through the computer and enabling the verification of the information preferably with a validation centre, before allowing the user to connect

to the network.

Viewed from a further aspect, the present invention provides an interface apparatus for allowing a computer to access a network, wherein the apparatus mimics a connection to the network by the computer to allow an application related to the network to be launched, and prompts the user for validation information through the use of this application.

Thus, instead of basing the interface apparatus on the use of a browser, an alternative application may be used, e.g. E-mail. In this case, E-mails may be sent between the computer and interface, and any necessary information may be extracted from the E-mails.

Viewed from a still further aspect, the present invention provides an interface apparatus for allowing a computer to access a network, wherein the interface apparatus mimics a connection to the network by the computer, obtains validation information from the user, and allows the computer to connect to the network when the validation information is determined to be correct.

Viewed from a further aspect, the present invention provides an apparatus for allowing a computer to connect to a network, the apparatus obtaining card information from the user and enabling the card information to be checked at a clearing card organisation before allowing access to the network.

Viewed from a further aspect, the present invention provides apparatus for allowing a computer to connect to a network, the apparatus requesting validation information from the user via the computer and checking the validation details e.g. with a clearing organisation before allowing the computer access to the network.

Viewed from a further aspect, the present invention provides an interface apparatus which allows the connection of a computer to a network, the interface apparatus mimicking a connection to the network by the computer and passing instructions to the computer to

obtain validation information from a validation centre and then to allow access to the network when validation is confirmed, at least the connection to the network being made by the modem of the computer.

Viewed from a further aspect, the present invention provides interface apparatus for allowing a computer to connect to a network, the apparatus including a modem for connection to a modem of the computer to exchange information therewith, the apparatus enabling a check of the user at a remote clearing organisation and then allowing the computer to connect to the network once the user is validated, the apparatus allowing at least the connection of the computer to the network to be through the computer's modem rather than through the modem of the apparatus, the apparatus preferably making an initial and a final connection with the clearing organisation, etc., using the modem of the interface apparatus.

Viewed from a further aspect, the present invention provides apparatus for connecting a computer to a network, the apparatus mimicking a requested IP address, downloading a HTML page to request card information, checking the information against the information obtained from e.g. a card swipe and then connecting the computer to the Internet if the card is verified as acceptable.

The term "computer" should be taken to include a standard PC or any other similar device, such as a Macintosh computer or for example a device having minimal computing ability, e.g. hard disc capacity, and having only a browser program, the device running appelets downloaded from the network. It may also include e.g. a television or other electronic apparatus having the necessary computing ability, and may include DSOD (digital service on demand) equipment.

An "intranet" should be taken to be any stand-alone network which works on a similar basis to the Internet

and uses e.g. a browser program for connection to it.

An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic diagram of a computer attached to a network through a telecommunications interface socket according to an embodiment of the present invention;

Fig. 2 is a flowchart of the connection procedure implemented by the interface and computer browser;

Fig. 3 shows a first screen which may be produced on the computer;

Fig. 4 shows a PIN number screen which may be produced on the computer;

Fig. 5 shows a validation screen which may be produced on the computer; and

Fig. 6 shows a rejection screen which may be produced on the computer.

Referring to Fig. 1, according to one embodiment of the present invention, a communications interface socket 1 comprises an onboard controller 2, a modem chipset 3, a RAM 4, an EPROM 5, a swipe card reader 6, a connection interface 7 to a line 8 of the local telephone network and a standard telephone plug socket 9.

The interface socket 1 allows a user of a computer 10 to connect to the Internet via a service provider 11.

All operations of the interface socket 1 are controlled through the onboard controller 2, the operating programs and other data for which are held in the EPROM 5. An EPROM 5 is used so that the program may be easily updated as necessary down line 8. For example, tariffs and contact telephone numbers may be easily refreshed in this manner.

The controller 2 may run a small and compact operating system, such as a Linix/Linux based operating system, Doslite or RomDos or the like, and the application program run to conduct the Internet

connection may be a Java-based program.

The interface socket 1 may for example be provided as one of a bank of such sockets in the lobby of a hotel or conference centre or in an airport lounge, and the computer 10 may be e.g. a laptop computer owned by a hotel guest, a visitor to an exhibition or conference or a person awaiting a flight.

To connect the computer 10 to the Internet, a user connects the computer's modem 12 to the plug socket 9 in the same manner as to a normal telephone socket using a standard telephone cable 13. This prompts the socket to wake up and enact the routine shown in Fig. 2.

Firstly, in Fig. 2, the interface 1 waits for the plug-in of a connection line 13 from the computer 10, and, in step S1, the interface socket 1 runs an initialisation routine and resets its RAM on noting the plug-in. It then imitates a standard dial tone at step S2.

The socket 1 next awaits a connection request from the computer 10 at step S3, the connection request being sent by the computer 10 on initiation of the dial-up networking of the computer by the user - the modem 12 of the computer dialling the telephone number of e.g. the user's usual service provider.

The interface socket 1, in step S4, stores the telephone number dialled, and responds to the dial-up signal from the computer 10, using the chipset 3, by pretending that the socket 1 is the number dialled and by establishing the necessary handshaking, protocols, etc., with the modem 12. It then sends a dummy IP address to the computer 10 at step S5 in response to an IP assignment request. It also requests the user's username and password for its service provider and stores these in specific locations in its RAM 4. The computer thus believes that it has accessed a service provider and obtained a connection to the Internet.

Socket 1 then awaits the launch of the computer's

browser and an URL request from the browser at step S6 and stores this requested URL at another location in the RAM 4.

The socket 1 then downloads HTML code at step S7, the code comprising a html page including a JAVA™, JAVASCRIPT™ and/or ACTIVEX™ appelet stored in the EPROM 5.

The appelet is interpreted/run by the browser to provide prompts to the user and to control the computer during the subsequent connection procedures.

The first html page prompts the user to swipe their card through the card swipe 6, and produces a screen as shown in Fig. 3.

The socket 1 is at this time set at step S8 to await data from the swipe card reader 6.

Once a card is swiped through the reader 6, the interface socket 1 captures the card data and logs it to predefined memory locations in the RAM 4 at step S9.

The data is checked for completeness at step S10, and further prompts are used as required to collect any additional data needed to gain validation by sending further html pages as appropriate to the computer. The Java program running on the interface controller 2 attempts to fill a database of user information required for the card, and prompts the user for further inputs until all the required fields are filled.

An example of a further information screen is shown in Fig. 4, which in this case requires the input of the user's card PIN number. Other screens may also be provided as necessary. For example, the interface may check that the card is supported and can be validated by the interface, and, if not, may issue a html page (not shown) to indicate the need for an alternative card or to exit the log on. In this case, it will also signal the interface to await a new card swipe.

When all information is complete, the interface socket 1 instructs the browser (which is running the

initially downloaded applet) to await further information as step S11, and hangs up the connection with the computer at step S12.

The interface then dials the appropriate card clearing organisation 14, at step S13, through its modem chipset 3, and sends the card data to the clearing organisation and obtains authorisation to use the card. The interface then charges a certain fee to the card swiped as a "reserve" amount, which allows for a set minimum amount of connection time on the Internet according to the specific tariff being used by the interface owner.

The interface may also download information to permanent storage media for accounting/reporting purposes, such as the identity of the user and the time of access, etc.

Once the card clearing organisation has issued an acceptance or decline signal to the interface, the interface hangs up the connection at step S14, and reconnects to the computer, at which time it sends a signal to the browser that the further information awaited is ready to be transmitted.

Depending on the result of the authorisation query with the clearing organisation, either the screen of Fig. 5 or the screen of Fig. 6 may be displayed. If the card is invalid, the screen 6 is displayed and the connection is terminated. Alternatively, access could be allowed, as below, but suitable authorities, etc., could be alerted to the invalid use, so that the user may be apprehended.

If the card is accepted, screen 5 is displayed, and the browser then receives any data necessary for connection to the Internet (e.g. the username, password, dial-up number and/or desired URL) from the interface at step S15.

The interface then hangs up the connection at step S16, and the interface actuates e.g. a relay to allow

for direct connection of the computer to the telephone line. The interface also begins to monitor the line to await for a disconnection, and starts a timer for determining a time-out corresponding to the amount of time paid for by the reserve payment charged at step S13.

The browser run program next instructs the computer's modem 12 to connect to a service provider at step S17. This may be either a default service provider associated with the socket 1 or the service provider initially dialled by the user. In the latter case, the service provider's telephone number, and the username and password of the user will have been obtained from the RAM 6 of the socket 1 at step S15 in order to allow the connection without the need for the user to re-enter these. Alternatively, the user may be prompted to re-enter his username and/or password in the usual manner, or the browser can use defaults already stored in the computer's dial-up networking.

When either the time-out occurs or the user disconnects from the Internet, the socket 1 contacts the card organisation at step S18 and makes a charge for the overall amount spent, if e.g. less than that originally charged as the reserve amount. At disconnect by the time-out, the user may be asked if they wish to continue with the connection, and, if they do, a further "reserve" amount may be charged to the user's card, or the time used may be charged at the end of the connection as a top-up fee.

After contacting the clearing organisation (or after the user decides not to continue after a time-out), the socket 1 powers down at step S19 and goes into standby mode to await a new connection.

As said, the above interface apparatus may be especially useful in for example hotels and conferencing facilities, where a bank of such interface sockets may be provided. A user need then only connect their

computer to one of the sockets and begin work, whilst being billed directly through their credit card and without the need for example to have a room number against which their call to the service provider can be billed. The interfaces may be used in any other suitable establishments, such as cafes, which provide Internet access on payment of a fee.

The charges made on the credit card may be e.g. by the hotel or conference centre providing the interface, and may include the telephone line time charge at a standard rate or at a rate increased to provide some profit to the socket provider, as well as a fee for the use of the socket. A charge may also be made by a service provider associated with the socket for e.g. online time and/or a connection fee.

The above is only one embodiment of the present invention, and various alternatives are possible. For example, instead of using a socket 1, the apparatus may be a separate free-standing device which connects between the computer and a standard telephone socket. Alternatively, the device may be mounted in the computer as an add-on. Also, the telephone line may be an ISDN or POTS line.

Instead of being used to connect to the Internet, the invention may be used to connect to an intranet of e.g. a large company, the credit cards in this case may be replaced by security cards whose details are checked with a security centre before allowing the network access.

Instead of using the computer's browser application, a different application may be used. For example, the connection routine may take place using E-mail between the interface and the computer, with instructional messages being sent to the computer via E-mail and the validation data such as a PIN number being transmitted as return E-mail from which the necessary information may be extracted by the interface.

Instead of using the interface with a computer, the interface may allow for connection with any other type of device needing communication with any other type of network, and may relate to e.g. televisions equipped with Internet access or DSOD equipment.

Instead of using a magnetic swipe card, the validation information could be in any other suitable form, and could be in the form of a smart card or physical information from the user, such as a palm, finger or eye print. In either case, a suitable reader would replace the swipe reader.

Also, there may be no need to contact with a central clearing organisation or security centre, if the validation data can be held on e.g. a card and checked by the interface with information input by the user.

If desired, the interface could output a receipt of e.g. time used, amount charged, etc.

Instead of using a single modem chipset on the interface, two modem chipsets could be used, so that the interface need not hang up on the computer in order to connect to e.g. a card clearing organisation.

Instead of waiting for the user to operate the browser, the interface may download instructions for autoloading the browser or other application or may initiate a screen with instructions to the user to launch the required application.

The initial connection to the card clearing organisation could be made by the modem of the computer on instruction from the downloaded appelet, so that the interface modem need only make the final connection to the clearing organisation.

Claims

1. Interface apparatus for allowing a computer to connect to a network, wherein the apparatus in use mimics a connection to the network by the computer so that the computer is able to launch an application for the network, the apparatus downloading a program or other coding to the computer to be run/interpreted by the application to obtain validation data from the user, the computer being allowed access to the network when the validation data is determined to be valid.

2. The apparatus of claim 1, wherein a connection is made to a remote validation centre for validating the user.

3. The apparatus of claim 2, wherein the validation centre is a card billing centre or a security authorisation centre.

4. The apparatus of claim 2 or 3, wherein the connection to the validation centre is made by the interface apparatus.

5. The apparatus of claim 2 or 3, wherein the connection to the validation centre is made by the computer.

6. The apparatus of any preceding claim, wherein when the data is validated, the interface allows the computer to connect directly with the network.

7. The apparatus of any preceding claim, wherein the interface apparatus monitors the connection to the network, and, on disconnection, contacts a billing or other remote centre.

8. The apparatus of any preceding claim, wherein the validation data includes data associated with a credit, debit, charge, security, or other card.

9. The apparatus of any preceding claim, wherein the validation data includes a physical characteristic.

10. The apparatus of any preceding claim, wherein the validation data includes a PIN number.

11. The apparatus of any preceding claim, wherein the application is a browser, and wherein the interface apparatus downloads NTML code to the browser to provide prompts to the user for obtaining validation data.

12. The apparatus of any of claims 1 to 10, wherein the application is E-mail.

13. The apparatus of any preceding claim, wherein the apparatus presents a dial tone to the computer when a modem of the computer is connected to it.

14. The apparatus of claim 13, wherein the apparatus replies to the computer as if it is a modem of a service provider of the network, and an IP address is provided to the computer to allow the application to launch.

15. The apparatus of claim 14, wherein the apparatus stores for later use information regarding user connection details sent from the computer.

16. The apparatus of claim 14 or 15, wherein the apparatus sends a prompt to the application to prompt a request for the user's validation data, and the interface is directed to look for an input of the validation data.

17. The apparatus of claim 16, wherein the interface obtains validation data from a card swipe reader.

18. The apparatus of any preceding claim, wherein the apparatus downloads code to the application to control the operation of the interface during later stages of the connection procedure, then disconnects from the computer and connects with a validation centre, whilst the computer application is instructed to await further information; wherein once the user is validated, the interface disconnects from the validation centre, and reconnects with the computer and provides any information necessary to log onto the network; and wherein the application then disconnects from the interface apparatus and connects to the network, the interface apparatus operating switch means to allow for access to the telephone system by the computer.

19. The apparatus of claim 18, wherein the computer connects to either the service provider initially called by the user or to a service provider associated with the socket, and the computer connects either with an URL address previously or presently requested by the user or with an URL address stored in the interface apparatus.

20. The apparatus of any preceding claim, wherein the apparatus is in the form of a wall socket.

21. The apparatus of any of claims 1 to 19, wherein the apparatus is provided as a stand alone unit which connects with both the computer and a telephone socket.

22. The apparatus of any of claims 1 to 19, wherein the apparatus is mounted within the computer.

23. A method of allowing the connection of a computer to a network by providing an interface between the computer and the network, the interface enabling validation information to be obtained from the user through the computer and enabling the verification of the information, before allowing the user to connect to the network.

24. The method of claim 23, wherein verification is carried out by connection with a remote validation centre.

25. An interface apparatus for allowing a computer to access a network, wherein the apparatus mimics a connection to the network by the computer to allow an application related to the network to be launched, and prompts the user for validation information through the use of this application.

26. The apparatus of claim 25, wherein the application is E-mail.

27. The apparatus of claim 25, wherein the application is a browser.

28. An interface apparatus for allowing a computer to access a network, wherein the interface apparatus mimics a connection to the network by the computer, obtains validation information from the user, and allows the computer to connect to the network when the validation information is determined to be correct.

29. An apparatus for allowing a computer to connect to a network, the apparatus obtaining card information from the user and enabling the card information to be checked at a clearing card organisation before allowing access to the network.

30. Apparatus for allowing a computer to connect to a network, the apparatus requesting validation information from the user via the computer and checking the validation details before allowing the computer access to the network.

31. An interface apparatus which allows the connection of a computer to a network, the interface apparatus mimicking a connection to the network by the computer and passing instructions to the computer to obtain validation information from a validation centre and then to allow access to the network when validation is confirmed, at least the connection to the network being made by a modem of the computer.

32. Interface apparatus for allowing a computer to connect to a network, the apparatus including modem means for connection to a modem of the computer to exchange information therewith, the apparatus enabling a check of the user at a remote clearing organisation and then allowing the computer to connect to the network once the user is validated, the apparatus allowing at least the connection of the computer to the network to be through the computer's modem.

33. The apparatus of claim 32, wherein the apparatus makes an initial and/or a final connection with the clearing organisation using the modem of the interface apparatus.

34. Apparatus for connecting a computer to a network, the apparatus mimicking a requested IP address, downloading a HTML page to request card information, checking the information against information obtained from a user and then connecting the computer to the Internet if the card acceptable.

The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 9801413.7	**Examiner:**	David Keston
Claims searched:	1-22, 25-28, 31, 33 & 34	**Date of search:**	25 August 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP); H4K (KOD5, KOD6)

Int Cl (Ed.6): G06F 1/00; G07F 7/08, 7/10, 7/12; H04L 9/32

Other: Selected publications and online: COMPUTER, EDOC, JAPIO, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	US 4876717 (AT&T) - see whole document	1-34

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.